REMARKS

Please enter the above amendments prior to consideration of the merits of the present application.

Copies of the amended portion of the specification with changes marked therein is attached and entitled "Version with markings to show changes made."

Respectfully submitted,

Takashi KOBAYASHI

THE COMMISSIONER IS AUTHORIZED TO CHARGE ANY DEFICIENCY IN THE FEES FOR THIS PAPER TO DEPOSIT ACCOUNT NO. 23-0975

By: Michael S. Huppert

Michael S. Huppert
Registration No. 40,268
Attorney for Applicant

MSH/jz
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
August 1, 2001

Version with Markings to Show Changes Made

P25383-01 (Amended English version)

~~Information Processing system and Method strengthen in Password~~

INFORMATION PROCESSING SYSTEM HAVING FORTIFIED PASSWORD FUNCTION AND METHOD THEREOF

BACKGROUND OF THE INVENTION

FIELD OF THE INVENTION

The present invention relates to information processing system and a method of processing the information, and more specifically it relates to a technique of processing information to improve benefit and convenience of the operator, and to ensure security of the recorded information.

DESCRIPTION OF THE PRIOR ART

With the wide use of information processors in recent years, value of information themselves recorded in secondary memories are becoming far greater than value of main bodies of the information processors. Since the secondary memories are removable in general, there is a risk that the recorded information is used illegitimately by third parties who have stolen them. Thus, there are demands for security techniques that render the information in the secondary memories not readable by even the third parties who have stolen them.

Information processors and information processing systems of the prior art, when stolen, can be disassembled so as to take out secondary memories therefrom. When this happened, the information is not prevented from an illegitimate using by means of only a password used for startup if any of the removed secondary memories is connected to another information processor and used wrongfully. For this reason, in the conventional information processors, upon removing the information recorded in the secondary memories are rendered not useable even by setting different passwords

drive (FDD), a compact disk read only memory device (CD-ROM), a compact disk recording device (CD-R), a compact disk read/write device (CD-R/W), a compact disk random access memory device (CD-RAM), a digital video disk read only memory device (DVD-ROM), a digital video disk recording device (DVD-R), a digital video disk read/write device (DVD-R/W), a digital video disk random access memory device (DVD-RAM), a digital tape recording device, or the like, besides the hard disk drive (HDD). Moreover, there may be such cases that the secondary memory 6 is integrated into the main unit of the information processor, and it is separated from the main unit of the information processor in a removable manner. Furthermore, the secondary memory 6 is normally removable even if it is integrated with the main unit of the information processor.

Fig. 2 is a process flowchart during startup of the basic input-output system (BIOS) in the present exemplary embodiment.

In Fig. 2, a power-on step 21 is for turning on the power supply of the information processing system. The information processing system then starts executing the basic input-output system (BIOS) 2. AtA recorded password check step 22, CPU 1 ~~is for~~ checksing the nonvolatile memory 5 and the secondary memory 6. CPU 1 ~~it~~ determines whether or not the startup password for starting the information processing system, and the secondary password for the secondary memory 6 ~~is~~are stored in any of them. If the startup password and the secondary password are stored in any of the nonvolatile memory 5 and the secondary memory 6, a state of the system passes on to an input means check step 24. If ~~the startup password and~~the startup password and the secondary password are not stored in the nonvolatile memory 5 and the secondary memory 6, the state of the system passes on to a password setting display step 23, and displays a ~~startup password and~~startup password and secondary password setting screen in the display device 4 such as a CRT or a liquid crystal display representing the display means, and urges the operator to set ~~a startup password and~~a

startup password and a secondary password. In this password setting display step 23 here, the display device ~~6~~ 4 may be substituted by a vocal means, in place of the screen display, to produce vocal sound for urging the operator to set ~~the startup password and~~the startup password and the secondary password with the voice.

The input means check step 24 is for detecting whether or not an input device 3, or the input means, such as a keyboard, for example, is connected to the main unit of the information processor. The state of the system goes on to a password input request step 25, if the input device 3 is connected to the main unit of the information processor. If no input device 3 is connected to the main unit of the information processor, the state of the system goes on to a password acquisition step 26, and acquires the secondary password for the secondary memory 6 stored in the nonvolatile memory 5. Then, the state of the system goes on to a password security unlock step 28. The password input request step 25 is materialized by displaying a password input setting screen in the display device 4, or the display means such as a CRT, a liquid crystal display and the like, for instance. The state of the system goes on to a password matching step 27 when the operator inputs a startup password according to the password input setting screen .

Here, a vocal means may be used in place of the display means to urge the operator to set the startup password with the voice.

The password matching step 27, there is checks whether or not the startup password and the secondary password input in the password input request step 25 matches with the startup password and the secondary password for the secondary memory 6, stored in the nonvolatile memory 5 and the secondary memory 6. If the input secondary password is in agreement with the secondary password stored in the nonvolatile memory 5 and the secondary memory 6, the state of the system goes on to the password security unlocking step 28. If the startup password and the input secondary password is in discordance with those stored in the nonvolatile memory 5 and the secondary memory 6, the state of the system goes on to a startup process

interrupting step 210, where the discordance interrupts starting process of the entire information processing system or the main unit of the information processor.

The password security unlocking step 28 is for setting within the secondary memory 6 either the startup password which is input in the password input request step 25, or the secondary password acquired in the password step 26. That is, the password security unlocking step 28 unlocks the security lock of the main unit of the information processor and the information processing system based on the accordance of startup password, in the case the input device 3 is connected and fair startup password is input by the operator. And it also unlocks the security lock of the main unit of the information processor and the entire information processing system based on the acquired secondary password from the password acquisition step 26. Upon unlocking the security lock, the state of the system goes on to a startup process continuation step 29 to continue the starting process of the entire information processing system or the main unit of the information processor.

If the secondary memory 6 is removed, and then connected to another information processor of the same model but different from the main unit of the information processor in which the secondary password is set, this another information processor checks whether or not the secondary password for this removed secondary memory 6 is stored in a nonvolatile memory 5 within the another information processor and the removed secondary memory 6. If the secondary password is stored in the nonvolatile memory 5 and the secondary memory 6, the state of the system goes on to the input means check step 24. If the secondary password is not stored in the nonvolatile memory 5 of the another information processor and the secondary memory 6, the state of the system goes on to a password input setting display step 23, and displays a startup password and a secondary password setting screen in a display device 4 defining display means such as a CRT or a liquid crystal display, and urges the operator to set a secondary password. At this step, an illegitimate operator is able merely to input a random startup password and a random secondary password, since

he/she has no knowledge of the secondary password especially for this removed secondary memory 6. Thus, the random secondary password input here cannot match with the secondary password stored in the nonvolatile memory 5 and the secondary memory 6 except for an accidental case. The state of the system hence goes on to the startup-process interrupting step 210, where the input of random passwords result in interrupting the starting process of the entire information processing system or the main unit of the information processor. Accordingly, this contrivance protects the information kept in the removed secondary memory from unfair use.

Further, when the main unit of the information processor and the secondary memory 6 are removed together, and connected to another display device different from the original one, the information stored in the secondary memory 6 becomes readable only through this another display so long as no input device is connected. However, the illegitimate operator cannot tamper with the information itself stored in the secondary memory 6, and also he/she cannot use it unfairly for any other purposes and means. Since this fact has been made clear in the foregoing explanation, further details will be skipped here.

As has been described in details as above, the information processing system of the present invention avoids the inconvenience of inputting the password every time the operator uses it, since the information processor starts automatically, so as to thereby display automatically the information stored in the secondary memory 6 in the display device 4, when the input device 3 is not connected to the information processor. In addition, the present invention can minimize the risk of information leakage if the information processor, the secondary memory, and the like are stolen. In other words, if there is a password set with it, and if it is not connected with an input device capable of inputting a password, it starts the information storage device irrespective of presence or absence of the password, and provides the display device with the information of the secondary memory, thereby improving convenience of the operator. Moreover, if

said main unit of the information processor regardless of a result of determination of said startup password presence checking means;

a startup condition judging means for making a judgement as to whether or not the startup condition stored in said startup condition storage means is satisfied; and

a main unit starting means for starting said main unit of the information processor when a result of determination of said startup condition judging means satisfies the startup condition.

3. The information processing system as set forth in [any of] claim 1 ~~and claim 2,~~ wherein:

said main unit of the information processor further comprises an input means connection detecting means for detecting whether or not an input means is connected to said main unit of the information processor; and

a startup condition for said main unit of the information processor is satisfied when a detected result of said input means connection detection means indicates no connection.

4. The information processing system comprising:

a secondary memory;

a password setting means for setting a secondary password for said secondary memory;

a secondary password storage means for storing said secondary password;

a secondary password presence checking means for determining whether or not said secondary password for said secondary memory is stored in said secondary password storage means; and

a secondary password request means for requesting setting with an input means of a secondary password for said secondary memory when a result of determination of said secondary password presence checking means indicates absence

of the secondary password.

5. The information processing system as set forth in claim 4, further comprising:

a security unlock condition storage means for storing a security unlock condition used for unlocking a secondary password protection for said secondary memory, irrespective of a result of determination of said secondary password presence checking means;

a security unlock condition judging means for making a judgement as to whether said security unlock condition stored in said security unlock condition storage means is satisfied; and

a secondary password security unlocking means for unlocking said secondary password protection for said secondary memory when a result of determination of said security unlock condition judging means satisfies said security unlock condition.

6. The information processing system as set forth in [any of] claim 4 ~~and claim 5~~, further having an input means connection detecting means for detecting whether said input means is connected, wherein

a security unlock condition is satisfied when a result detected by said input means connection detecting means indicates no connection.

7. The information processing system as set forth in claim 4, wherein said secondary memory is removable from said main unit of the information processor.

8. The information processing system as set forth in [any of] claim 1 ~~and claim 2~~, wherein said startup password request means includes a display means.

9. The information processing system as set forth in any of claim 4 ~~and claim 5~~, wherein said secondary password request means includes a display means.

10. The information processing system as set forth in claim ~~8~~, wherein said display means further includes a supplementary input means provided with a touch panel.

11. The information processing system as set forth in claim ~~9~~, wherein said display means further includes a supplementary input means provided with a touch panel.

12. The information processing system as set forth in claim 1, wherein said startup password request means further includes a voice generation means for requesting setting of a startup password with vocal sound produced by said voice generation means.

13. The information processing system as set forth in claim 4, wherein said password request means further includes a voice generation means for requesting setting of a secondary password with vocal sound.

14. The information processing system as set forth in claim 7, wherein, if said secondary memory provided with a secondary password set therein is connected to another information processor different from said information processor, and when said another information processor is connected with an input means, said another information processor starts only when an password identical to said secondary password set therein is input from said input means.

15. The information processing system as set forth in claim 7, wherein, if

as to presence or absence of said startup password in storage;

determining whether or not said stored startup condition is satisfied; and

starting said main unit of the information processor when said startup condition is satisfied.

18. The method of processing information as set forth in any of claim 16 ~~and claim 17,~~ further comprising the steps of:

detecting whether or not said input means is connected to said main unit of the information processor; and

starting said main unit of the information processor under a condition that said detected result indicates said input means not in connection thereto.

19. A method of processing information for information processing system having a secondary memory built into a main unit of information processor and a secondary password storage means for storing a secondary password for said secondary memory, said method comprising the steps of:

determining presence or absence of said secondary password in storage; and

requesting setting of a secondary password when said secondary password is absent.

20. A method of processing information for information processing system having a secondary memory removable from a main unit of information processor and a secondary password storage means for storing a secondary password for said secondary memory, said method comprising the steps of:

determining presence or absence of said secondary password in storage; and

requesting setting of a secondary password when said secondary password is absent.

21. The method of processing information as set forth in ~~any of~~ claim 19 ~~and claim 20,~~ further comprising the steps of:

storing a security unlock condition for unlocking protection of said secondary password for said secondary memory irrespective of presence or absence of a secondary password;

determining whether said security unlock condition is satisfied; and

unlocking the protection of said secondary password if said security unlock condition is satisfied.

22. The method of processing information as set forth in claim ~~21~~ 21, further comprising the step of detecting whether or not input means is connected, wherein

said security unlock condition is satisfied if said input means is not in connection.

23. The method of processing information as set forth in ~~any of~~ claim 16 ~~and claim~~ 17, further comprising the step of displaying a request for setting a startup password in a display screen.

24. The method of processing information as set forth in ~~any of~~ claim 19 ~~and claim 20,~~ further comprising the step of displaying a request for setting a secondary password in a display screen.

25. The method of processing information as set forth in claim 23, further comprising the step of inputting supplementary information by means of a display screen touched by an operator.

26. The method of processing information as set forth in claim 24, further comprising the step of inputting supplementary information by means of a display

screen touched by an operator.

27. The method of processing information as set forth in any of claim 16 and ~~claim 17~~, further comprising the step of requesting an operator to set a startup password with vocal sound.

28. The method of processing information as set forth in any of claim 19 and ~~claim 20~~, further comprising the step of requesting an operator to set a secondary password with vocal sound.